SiC-Chain: A simple, secure IoT System Architecture for small scale Cold Chain Applications

SYNOPSIS

Submitted for the award of the degree of

DOCTOR OF PHILOSOPHY

IN

COMPUTER SCIENCE AND ENGINEERING

by

DIVYA JAMES (Reg. No. 18PHEOP003)

Ph.D. Research scholar (Part Time)

Under the guidance of

Dr. TKS. LAKSHMI PRIYA

Professor

School of Engineering

Avinashilingam Institute for Home Science and Higher Education for Women

Coimbatore

August 2023

SiC-Chain: A simple, secure IoT System Architecture for small scale Cold Chain Applications

1. INTRODUCTION

Today, Internet of Things (IoT) envisions the autonomous interaction of pervasive and connected, smart nodes that can offer a myriad of services. IoT devices like sensors and actuators are deployed for collecting data from various sources. These devices can gather information about environmental conditions, machine performance and customer behaviour. Real-time data monitoring using IoT can offer valuable insights to enable prompt decision-making based on latest information. As IoT devices are increasingly prevalent in homes, businesses, and critical infrastructure, the IoT nodes are turning into a goldmine of data for malicious actors. Hence ensuring their security is essential to safeguard privacy, maintain operational integrity and prevent potential harm. Today, security and the detection of compromised nodes have become a major concern in IoT networks.

Supply chain management (SCM) encompasses all ensuing activities in the movement and management of materials, products, and information throughout the entire network. Its primary goal is to optimize the overall performance and competitiveness by reducing costs, enhancing customer satisfaction, and improving efficiency. Key components and activities involved in supply chain management include Planning, Sourcing, Production, Transportation, Warehousing, Inventory management, Distribution, Information systems, Risk management and Collaboration and Communication. SCM has become increasingly important in today's globalized and interconnected business environment. Effective supply chain management can result in improved efficiency, faster time-to-market, increased profitability, and greater resilience in the face of disruptions.

In temperature - controlled supply chain system or ‘cold chain network,’ some of the core challenges are impact of environment, security in cold chain network, insufficient temperature monitoring and maintenance system & absence of modern technology or optimal equipment.

Supply chain management (SCM) encompasses various activities and processes that can have environmental impacts throughout the entire supply chain. Temperature and humidity have significant effects on supply chain management, particularly in industries where temperature-sensitive or humidity-sensitive products are involved. Monitoring

temperature and humidity conditions throughout the supply chain is essential for maintaining product quality and ensuring compliance with regulations. Supply chain managers need to implement robust monitoring systems to track temperature and humidity levels at various stages, such as production, warehousing, and transportation. Real-time data monitoring and alert systems enable quick response to any deviations, allowing proactive measures to be taken, such as adjusting storage conditions or rerouting shipments to avoid unfavorable environmental conditions.

Security is a crucial concern in today's world, especially when it comes to digital data sharing. With the increasing reliance on digital systems and interconnected networks, data breaches have become a significant concern. Breaches in supply chain management systems can result in the theft of sensitive information. Conventional cryptography and lightweight cryptography are two approaches for securing information and communications, but they differ in terms of their design principles and target applications. Conventional cryptographic algorithms typically use larger key sizes and require significant computational resources, such as processing power and memory. They are often implemented on devices with sufficient resources, such as desktop computers, servers, or high-end mobile devices. Lightweight cryptography is specifically designed for resource-constrained environments, like embedded systems, Internet of Things (IoT) devices, and low-power microcontrollers. Its primary focus is on providing efficient and lightweight cryptographic solutions with a smaller code size, reduced memory requirement, and lower energy consumption. Lightweight cryptography offers efficient and lightweight solutions suitable for resource-constrained devices.

To meet the aforementioned requirements, a simple and secure IoT architecture for small-scale cold chain applications is required. In this research work, one such architecture is proposed for integrating IoT sensors with cloud technology for pervasive access of the real-time data in a cold chain environment. The proposed model is demonstrated with a simple web-based working model that has been developed and evaluated. For the security purposes, a dynamic key dependent security algorithm has been developed for which novel non-linear S-Boxes are generated using Logistic Chaotic Map and evaluated.

2. LITERATURE SURVEY

The Internet of Things (IoT) is a network of interconnected physical devices, appliances, and other objects embedded with sensors, software, and connectivity. These

devices can gather and exchange data over the internet, enabling interaction with their environment and with each other. IoT works on four different components like devices, gateways, cloud service and applications[1]. These work together for enabling collection, communication, processing, and analysis of data in IoT systems. The basic components, architecture and enabling technologies of IoT are discussed herewith.

Three-layer architecture is the basic layered architecture for IoT, comprising [2] of Perception layer, Network layer and Application layer. This helps in modularizing and organizing the IoT system, by making it more manageable, scalable, and flexible. It also facilitates the development of interoperable and reusable components, to enable faster deployment of IoT solutions and promote ecosystem growth. The Internet of Things (IoT) has varied applications across several industries. The essential features of Internet of Things (IoT) [3] in varied applications across several industries has been discussed. IoT's Technological components, can enhance the small-scale cold chain's efficiency, reduce risks, and ensure product quality throughout the supply chain.

Cryptography is a fundamental component of securing data and communications. This involves the use of mathematical algorithms and techniques to transform plaintext (original data) into ciphertext (encrypted data) and vice versa. There are several types of cryptography, [4] each serving different purposes and offering varying levels of security. Though the benefits are many when it comes to securing data and communications, this also brings with it certain limitations. [5]. A lightweight scheme based on the Addition substitution and XOR is proposed for the security of the e-healthcare system [6]. Many block cipher and stream cipher related lightweight algorithms are hereby proposed and evaluated [7]. The IoT security challenges, structure wise classification and the characteristics offered by Lightweight cryptography algorithms are defined and discussed [8] along with its performance parameters [9]. Fixed or static S-Box permits the attacker to explore S-Box and identify weaknesses of the algorithm. The inherent limitations of static S-Box used in Lightweight cryptography algorithms are elucidated [10]. Strength of this proposed S-box is analyzed by manipulating nonlinearity, differential approximation probability, linear approximation probability, strict avalanche criterion [11]. A systematic study is conducted to select, review, and synthesize the impact of cloud computing and supply chain integration [12].

A study on IoT-enabled process integration for supply chain management [13] is also highlighted, as are the basic issues in supply chain management [14]. However, a simple,

secure IoT architecture for small-scale cold chain applications is now unavailable. There are many commercially available [15] ERP software and third-party logistics for SCM Operations. Third-party logistics has limitations such as skilled talents and trustworthy third parties. NetSuite and Microsoft Dynamics 365 are Cloud based ERP software for small and mid-size business organizations. SAP S/4HANA Cloud is a fully integrated enterprise resource planning (ERP) system for large organizations with built-in cognitive technologies such as artificial intelligence (AI), machine learning, and advanced analytics. Infor Cloud Suite provide breadth of capabilities for specific industries like retail, healthcare organisations. The drawbacks of commercially available ERP software packages for SCM are expensive, vendor-dependent, time-consuming, and complex which are not suitable for small and medium sized B2B supply chain system models.

Suggested devices like paper-based temperature monitors can enable monitoring though the damage to sensitive indicators may fail to measure temperature.[16]. The use of dial thermometers and data loggers can monitor environmental factors, but the limitation is that these cannot provide real-time and instant data [17]. A general analytical framework to quantify the eavesdropping probability in wireless networks is proposed [18] and challenges in logistics applications are discussed [19]. An analysis of Fixed investment cost, tag price and shrinkage recovery rate including RFID and non-RFID cases is provided [20].

Studying the essential requirements [21] of supply chain management for small-scale cold chain applications involves understanding the unique challenges and considerations associated with maintaining the temperature-controlled storage and transportation of perishable goods in a limited-scale setting are discussed.

3. PROBLEM DEFINITION

Logistic constraints, inaccessible warehouses, and closed consumer outlets, during COVID-19 pandemic, have badly affected supply chains especially in small scale cold chain sectors. This brings out the need for simple and small-scale technological solutions that could monitor, manage, secure, and facilitate decision-making for reducing losses. The solution must be capable of making use of the IoT's in the pervasive smart phones that almost everyone in the unorganized sector of small businesses, is possessing. It must be able to integrate the power of cloud storage with the data handling capacity of hand-held devices via the Internet as the backbone in a feasible manner. Securing data becomes an essential requirement in such situations, thus simple security algorithms must be a part of the solution to be provided. Further for data collection during transit, smart

containers with sensors are to be made an integral part of the system. Small business firms could then monitor, track, and receive notifications about their goods as they moved along the cold chain.

4.OBJECTIVES OF THE RESEARCH

The primary objective is to model a simple, secure integrated IoT architecture which provides real-time data handling in a cold chain environment using a Cloud based web application.

The secondary objectives are:

- To evaluate and demonstrate the proposed architecture with a web-based working model.
- To propose a dynamic key dependent cryptographic algorithm for securing communication between IoT devices and web application.
- To generate and evaluate novel non-linear S-Boxes using Logistic Chaotic Map for the dynamic key dependent cryptographic algorithm.

5. RESEARCH METHODOLOGIES

The thesis work primarily involves the proposal of an IoT architecture for cold chain environment catering to small scale businesses in Indian scenario. The first step is the study of the essential requirements of supply chain management for small businesses dealing with goods that are temperature sensitive. The architecture will incorporate features like use of simple and easily available sensors-based systems, real-time data handling capabilities, web-based access to the system, mobile App for role-based access to the system for the end-users, and alerts and notifications regarding the goods in the supply chain.

The model is meant for small scale business and therefore does not include high-end IoT systems nor does it include the complete spectrum of precision sensors that are common in commercially available SCMs. Features that are essential for full-fledged commercial SCMs such as Fault tolerance, storage management, intensive data analytics, end-to-end security solutions, etc, are not considers essential for the given scenario, thus making the system simple, economical, and feasible for small businesses.

To demonstrate the architecture, a working model is developed for which a suitable implementation platform is first choosen. The platform has to be open source, asynchronous,

event driven, fast in code execution and provide a runtime environment for developing server-side web applications. The platform must be able to handle the IoT data in real-time, in a secure manner, must support a lightweight desktop environment and mobile end users, realtime data analysis and a database that is distributed and optimized for fast growing web and mobile apps.

In order to identify a suitable platform, an experimental setup of a simple IoT system with a few sensors is used for real-time, encrypted data collection and uploading to web based platform. This setup also includes a lightweight desktop environment for handling the sensors as well as for computational tasks. The setup along with the identified platform is then used for analysing the real-time data.

After testing the identified platform with real time values on the experimental setup, the platform is then subjected to larger data sets and a security algorithm is evaluated. Since no benchmark datasets exist for environmental parameters, the platform is demonstrated with a dataset consisting of sensor data with the experimental readings taken during multiple trails at different time intervals.

After testing with larger data sets, a full-fledged web-based application, with pairing mobile apps for end users, is developed and tested. The development platform is designed to handle the view layer used for development of both web and mobile applications. The performance evaluation for web application is analysed and average response time for transactions is calculated to verify acceptable performance levels.

After developing the platform and evaluating it, the next step is to develop a light weight security algorithm for secure communication between the IoT devices and the web application. Dynamic key dependent cryptographic algorithm is choosen for this purpose and performance evaluation parameters like strict avalanche effect, average encryption and decryption time, throughput, and memory consumption time are determined.

To further improve the secure web-based application thus developed, novel non-linear S-Boxes, the basic building boxes of the cryptographic algorithm, using Logistic Chaotic Map are generated. Performance analysis of S-Boxes are done on non-linearity, Differential Approximation Probability and Linear Approximation Probability.

Thus, a simple, secure IoT system architecture for cold chain applications is modelled, developed, and evaluated.

5.1 Proposed System Architecture- SiC-Chain

A simple secure integrated IoT architecture for cold chain industry is modelled along with its key features. The proposed architecture harnesses the power of the upcoming technologies (namely IoT's and Cloud) in order to make the SCM eco-system, a state-of-the-art system, which can overcome the challenges in the prevailing SCM systems. The key features of the proposed architecture include:

- **IoT-based architecture**: This feature enables data capturing, monitoring, and tracking in real-time, which makes the next stage decision systems more effective. With real-time tracking of various objects and data such as commodities in transit, data during acquisition, data during transmission, etc, challenges related to various aspects such as environmental issues, data integrity and reliability for small scale cold chain applications can be solved.

- **Role based access to the system:** Our proposed architecture, SiC-Chain can enroll the entities in cold chain. It works like an automation software. Suppliers, manufactures, wholesalers, retailers, and consumers can enroll in the application software. The entities can view, add the products, find the details, add favourite entities, make sell, and buy transactions.

- **Simple & Secure Architecture**: The architecture is simple and secure which models a security algorithm that provides end-to-end data protection from the sensing layer to the application layer to secure the communication between IoT devices and web-based working model.

- **Cloud-enabled Architecture**: In a cloud environment, storage and computing are no more a burden to the client nodes and therefore this feature enables even low-end hand-held devices like mobile phones and tablets, to become a part of the SCM eco-system.

This architecture is proposed as an integration of IoT and Cloud, for the cold chain applications and therefore named as SiC-Chain.

Our SiC-Chain architecture has four layers: Sensing layer, Networking layer, Middleware Layer and Application Layer. In cold chain entities, data sensing and collection tasks in real-time are carried out from the smart boxes in SiC-Chain sensing layer. The Internet of Things devices are trusted as each device in cold chain is authorized by the Device Type and unique Device ID. The real-time data from the sensors in the smart boxes are encrypted and passed to the SiC-Chain networking layer. This data is passed to the SiC-Chain middleware layer through the messaging protocol Message Queuing Telemetry Transport over WiFi via the SiC-Chain Network layer. SiC-Chain Middleware layer constitutes the cloud-based web services for storage of data in cold chain environment. In our architecture, SiC-Chain Application layer shares necessary interfaces like a smart real-time dashboard. This layer includes an intelligent platform or dashboard to view the decrypted real- time data and transaction data. All the Supply Chain Management entities can access the application through their smart phones, Personal Digital Assistant, and laptops.

For effective and smooth working of the SiC-chain environment, the following operations have been identified and formalized for the SiC-chain environment: (i) Enrollment (ii) Secure communication of data between the Internet of Things devices and platform

In our proposed architecture, suppliers, manufactures, wholesalers, retailers and consumers can enroll in the application. Supplier registers with the authentication service by providing email and password. The authentication service sends a token back to the supplier. This token along with user data is send to the server using an Application Programming Interface Call. The server extracts and validates the token with the authentication service. Once the token is validated, the user data is stored in the database. All the enrolled supply chain entities can view the dashboard. The authenticated suppliers can login and can do the insertion, fetching, sell and buy transactions by monitoring environmental parameters, tracking the GPS location in the dashboard. The sensor values are encrypted using a dynamic cryptographic algorithm specially mentioned for resource constrained devices. The encrypted values are stored in database and decrypted and can be viewed in smart dashboard.

5.2 Demonstrating the proposed architecture

Temperature and Humidity sensors are connected to Raspberry Pi which supports running in lightweight desktop environments. Using a high-level, general-purpose programming language python, the values are fetched and published in IBM Watson Internet of Things platform through Message Queuing Telemetry Transport protocol via

WIFI Client library. The Watson Internet of Things platform uses open-source Message Queuing Telemetry Transport protocol to allow devices and applications to connect to the Internet of Things platform. In order to secure communication between the devices and Internet of Things platform, a cryptographic algorithm is run, thereby encrypted data is sent to IoT platform. Node-RED, facilitates connection in the IoT infrastructure, can receive the data that was transmitted from the device over Message Queuing Telemetry Transport to Watson Internet of Things Platform. The data received via Node RED are stored in a persistent Cloudant database, which is distributed and optimized for fast growing web and mobile apps. From the Cloudant database, the decrypted data is fetched to the smart dashboard using Node.js which is open source, asynchronous and provides run time environment for server-side web applications. The SCM entities can register through the dashboard. The performance evaluation for SiC-Chain web application is analyzed. The average response time for transactions is calculated by using the request-responses collected from the SiC-Chain web application. Factors affecting response time are network bandwidth, user count, queries submitted. Performance test is executed and infinite iterations are considered. Even though we have increased the users from 100 to 1000, after performing the load test, web application is giving a consistent response time for supplier and manufacturer transactions.

5.3 Dynamic key dependent cryptographic algorithm

An S-box, a nonlinear auxiliary table, serves as the confusion component in encryption algorithm. From the generated non-linear S-Boxes, for each round the S-Box is selected based on a dynamic basis, which can be used to develop a newly defined dynamic key dependent algorithm to secure the communication between IoT devices and web-based platform for cold chain applications. The algorithm is developed and evaluated based on the performance parameters like average encryption/decryption time, throughput, Strict Avalanche effect & Memory Consumption. The throughput can be calculated using the formula: Throughput= No of bytes/Encryption Time measured in CPU clock cycles/sec.

5.4 Generation of non-linear S-Boxes using Logistic Chaotic Map

In cryptography, an S-box (Substitution-box) is a basic building block used in symmetric key algorithms, such as block ciphers. It is a fixed lookup table that performs substitution of elements from one representation to another. S-boxes introduce confusion and

non-linearity into the encryption process, increasing the algorithm's resistance to cryptanalysis. Fixed or static S-Box permits attackers to study S-Box and find weak points of the algorithm. Therefore, Non-linear S-Boxes are generated using Logistic Chaotic Map. Performance analysis has been done on Non-linearity, Differential Approximation Probability and Linear Approximation Probability.

The non-linearity property is typically evaluated by considering the difference distribution table or the Walsh-Hadamard transform of S-Box. Let Boolean function f be a bent function on F_2^4 then function f has maximum Nonlinearity [11] achieved when n is even of given by

$$N_f\ (\max) = 2^{n-1} - 2^{n/2-1}$$

Then this above Eq. shows that maximum non linearity achieved by these S-Boxes in GF (2^4) is 6.

The Differential approximation probability [11] of a given S-box is a measure for Differential Uniformity and is defined as:

$$DP(\Delta x \rightarrow \Delta y) = \frac{\#\{x \epsilon \frac{X}{S(x)} \oplus S(x \oplus \Delta x) = \Delta y\}}{2^n}$$

where Δx and Δy are input and output differentials for all the possible inputs 2^n

The Linear approximation probability [11] is the maximum amount of dissimilarity of an event and defined as:

$$\text{LP= max } \left| \frac{\#\{x/x.\Gamma x = S(x).\Gamma y\}}{2^n} - \frac{1}{2} \right|$$

Where Γ_x is input mask; Γ_y output mask and x input vector of all possible inputs 2^n

6. CONCLUSION

A simple, secure integrated IoT architecture is developed which provides real-time data handling in a cold chain environment. This enables entities in cold chain to take suitable decisions easily. The data between the IoT devices and platform has been securely transferred using a Dynamic key dependent algorithm. A cloud-based data processing and storage system, included with a user-friendly smart dashboard which can used for small scale cold chain applications. The performance analysis of SiC-Chain architecture is evaluated based on

the average response time of transactions. The performance evaluation of non-linear S-Boxes is evaluated based on non-linearity, Differential Approximation Probability, Linear Approximation Probability and Dynamic key dependent algorithm is evaluated based on strict avalanche effect, average encryption/decryption time, throughput, and memory consumption. The algorithm outperforms better than other algorithms for resource constrained devices.

7. ORGANIZATION OF THE THESIS

Chapter 1 describes overview, motivation, problem definition, research objectives and contributions. **Chapter 2** discusses existing studies on IoT architecture, challenges, cold chain, conventional cryptography, lightweight cryptography with their related limitations. **Chapter 3** explains the proposed integrated architecture along with its tools and technologies. **Chapter 4** describes generation of non-linear S-Boxes and its results. **Chapter 5** describes selection of dynamic key dependent S-Boxes, used to develop the novel cryptographic algorithm with its results. **Chapter 6** explains overall experimental evaluation results to prove effectiveness of proposed methods. **Chapter 7** concludes research findings with outlines for future enhancements and reference part with list of evidences used to explain the related concepts of the proposed methodology.

REFERENCES

[1] Choudhary, V., & Tanwar, S. (2023). A Concise Review on Internet of Things: Architecture and Its Enabling Technologies. Computational Intelligence for Engineering and Management Applications: Select Proceedings of CIEMA 2022, 443-456.

[2] Chaurasia, N., & Kumar, P. (2023). A Comprehensive Study on Issues and Challenges Related to Privacy and Security in IoT. e-Prime-Advances in Electrical Engineering, Electronics and Energy, 100158.

[3] Dadhaneeya, H., Nema, P. K., & Arora, V. K. (2023). Internet of things in food processing and its potential in industry 4.0 era: A review. Trends in Food Science & Technology.

[4] Ahmed, S., & Ahmed, T. (2022). Comparative Analysis of Cryptographic Algorithms in Context of Communication: A Systematic Review.

[5] Chander, S. (2022). Lightweight Cryptography Algorithms for Security of IoT Devices: A Survey. IRJET, 842-850.

[6] Chatterjee, Kakali, Ravi Raushan Kumar Chaudhary, and Ashish Singh. "A lightweight block cipher technique for IoT based E-healthcare system security." Multimedia Tools and Applications 81.30 (2022): 43551-43580.

[7] Rana, M., Mamun, Q., & Islam, R. (2022). Lightweight cryptography in IoT networks: A survey. Future Generation Computer Systems, 129, 77-89.

[8] Thakor, V. A., Razzaque, M. A., & Khandaker, M. R. (2021). Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities. IEEE Access, 9, 28177-28193.

[9] Panahi, P., Bayılmış, C., Çavuşoğlu, U., & Kaçar, S. (2021). Performance evaluation of lightweight encryption algorithms for IoT-based applications. Arabian Journal for Science and Engineering, 46, 4015-4037.

[10] Mostafa, S. M., Darwish, I. M., & Saadi, M. R. (2020). Improved lightweight security approach routing protocol in internet of things. Internet of Things, 11, 100208

[11] Shah, T., & Qureshi, A. (2019). S-box on subgroup of Galois field. Cryptography, 3(2), 13.

[12] Novais, L., Maqueira, J. M., & Ortiz-Bas, Á. (2019). A systematic literature review of cloud computing use in supply chain integration. Computers & Industrial Engineering, 129, 296-314.

[13] De Vass, T., Shee, H., & Miah, S. J. (2018). The effect of "Internet of Things" on supply chain integration and performance: An organisational capability perspective. Australasian Journal of Information Systems, 22.

[14] Zhang, Y., Zhao, L., & Qian, C. (2017). Modeling of an IoT-enabled supply chain for perishable food with two-echelon supply hubs. Industrial Management & Data Systems, 117(9), 1890-1905.

[15] Haddara, M., Gøthesen, S., & Langseth, M. (2022). Challenges of cloud-ERP adoptions in SMEs. Procedia computer science, 196, 973-981.

[16] Vrat, P., Gupta, R., Bhatnagar, A., Pathak, D. K., & Fulzele, V. (2018). Literature review analytics (LRA) on sustainable cold-chain for perishable food products: research trends and future directions. Opsearch, 55, 601-627.

[17] Ashok, A., Brison, M., & LeTallec, Y. (2017). Improving cold chain systems: Challenges and solutions. Vaccine, 35(17), 2217-2223.

[18] Dai, H. N., Wang, H., Xiao, H., Li, X., & Wang, Q. (2016, August). On eavesdropping attacks in wireless networks. In 2016 IEEE Intl Conference on Computational Science and Engineering (CSE) and IEEE Intl Conference on

Embedded and Ubiquitous Computing (EUC) and 15th Intl Symposium on Distributed Computing and Applications for Business Engineering (DCABES) (pp. 138-141). IEEE.

[19] Tadejko, P. (2015). Application of Internet of Things in logistics–current challenges. Ekonomia i Zarządzanie, 7(4), 54-64.

[20] Fan, T., Tao, F., Deng, S., & Li, S. (2015). Impact of RFID technology on supply chain decisions with inventory inaccuracies. International Journal of Production Economics, 159, 117-125.

[21] Mohan, A., Krishnan, R., Arshinder, K., Vandore, J., & Ramanathan, U. (2023). Management of postharvest losses and wastages in the Indian tomato supply chain- a temperature-controlled storage perspective. Sustainability, 15(2), 1331.

LIST OF PUBLICATIONS

1. Divya James & Dr.TKS Lakshmi Priya. (2020). Improving the product services using IoT for controlling in-transit parameters. *Our Heritage,* ISSN 0474-9030, Vol-68, Issue-44. (UGC-CARE)
2. Divya James & Dr.TKS Lakshmi Priya. (2023). "An integrated IoT architecture to monitor nutrient level along the food supply chain." *Indian Journal of Nutrition and Dietetics*, Online ISSN: 2348-621X, Vol.60, No.1. (UGC-CARE)

LIST OF CONFERENCES ATTENDED

1. Divya James, Alagusundari.N, Dr.TKS Lakshmi Priya, "A top-down Survey on Security Aspects of the IoT" in International Conference on Recent Scientific Research in Engineering and Technology, 22nd March 2019.
2. Divya James, Dr.TKS Lakshmi Priya, "An IoT based traceability framework for small scale farms" in 2nd International Conference on Emerging Technologies in Data Mining and Information Security,2nd - 4th July 2020 and published in Springer Advances in Intelligent Systems and Computing (AISC) Series, ISBN-978-981-15-9926-2, June 2021. (Scopus)
3. Divya James, Dr.TKS Lakshmi Priya: "Security enabled IoT architecture for cold chain packaging applications" in International Conference on Emerging Trends in Industry 4.0 and Sustainable Concepts, at Avinashilingam Institute for Home Science and Higher Education for Women 24-25 February 2023.